Deep Neural Network-Based Trust Models for Securing Interconnected Transportation Systems in Sustainable Cities

Md Shahbaz Alam
M.Tech Scholar
Department of Computer Science and Engineering
Technocrats Institute of Technology and Science
Bhopal, Madhya Pradesh, India
myselfalamshahbaz15@gmail.com

Mukesh Asati
Assistant Professor
Department of Computer Science and Engineering
Technocrats Institute of Technology and Science
Bhopal, Madhya Pradesh, India

Rakesh Kumar Tiwari
HOD
Department of Computer science and Engineering
Technocrats Institute of Technology and Science
Bhopal, Madhya Pradesh, India

***Abstract*:** This study elaborates on a hybrid model of deep learning for detection and classification of malicious behaviour in a transportation system in order to ensure security in smart cities. The model consists of Neural Networks (NN) for spatial feature extraction; XGBoost for temporal analysis; and an Attention mechanism to prioritize data points that are important, improving the model's focus on critical features such as trust degree and vehicle location. By utilizing SMOTE, the model addresses the class imbalance so that under-learning of even the poorly represented attack types like DoS, Whitewash, and Brute-force be alleviated. It effectively learns the spatial-temporal patterns of the vehicle behaviour, thus providing a broader perspective of attacks evolving over time. Performance evaluation is conducted using standard classification metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC, which yield satisfactory results demonstrating that the model is highly accurate in classification as well as detecting malicious behaviour with low false positives. Further, the attention mechanism refines predictions through focus on the most important features. Thus, it is promising, scalable, and dependable in real-time attack detection and continuous monitoring in transportation systems, towards developing secure, resilient smart city infrastructure with a much greater emphasis on security and sustainability.

Keywords: Hybrid Model, Deep Learning, Neural Networks (NN), XGBoost, Attention Mechanism, Synthetic Minority Over-sampling Technique (SMOTE), Class Imbalance, Attack Detection, Transportation Systems, Smart Cities, Malicious Behavior, DoS Attack, Whitewash Attack, Brute Force Attack, Real-time Monitoring, Security,

I.INTRODUCTION

Smart cities represented an advanced model of urban development, seeking to use advances in information and communication technologies, otherwise referred to as ICTs, together with advanced applications of the Internet of Things, to improve the quality of life for residents, the city as a whole operates, as well as with regard to the sustainable benefits now and into the future. They will be collecting and applying extensive networks of sensors and smart devices on systems related to transport, energy consumption, public safety, and waste. It is the catalyst behind all of this and the means through which all of that would be data-enabled decision-making by urban planners and managers. The upsurge in the evolution of smart cities would be propelled by a concomitant rise in urbanization that calls for a new approach to resource and infrastructure management within the urban environment, transforming entirely the nature of functioning within cities as well as human affiliations with their environment [1].

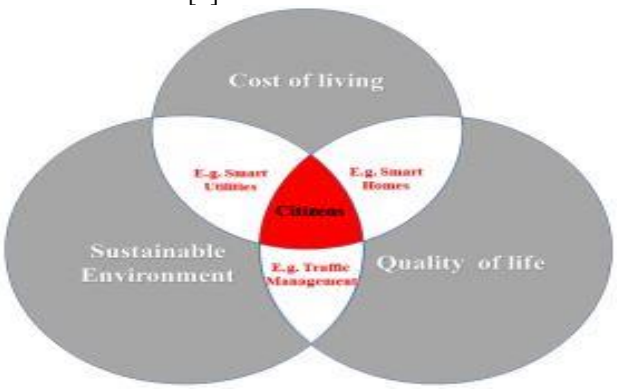

Figure 1 Fundamental models of Smart cities [2]

Figure 1 the rapid growing of information and assets are essentials for smart cities of being on the top of millions of real-time reacting and communicating devices [2]. The Internet of Things (IoT)- the term coined at MIT in 1999- refers to a world of global networks of exchanges between devices capable of autonomous information processing or decisions. That propels a paradigm shift that has allowed for the emergence of intelligent systems based on miniaturized high-performance electronics with cheap, widespread high-speed internet. In the case of smart cities, an example of the role of IoT as a disruptive paradigm of communication is that it connects different forms of digital devices to the internet to enable innovative, continuous urban applications [3]. IoT architectures, protocols, and enabling technologies have been explored in many studies, like Bhopal smart city project, which illuminates service development in areas like noise monitoring. IoT service characterization of smart cities is increasingly inclined to treat devices within the smart city as service providers similar to cloud systems,

allowing for higher-level abstractions and smoother integration between physical infrastructure and cloud services [4].

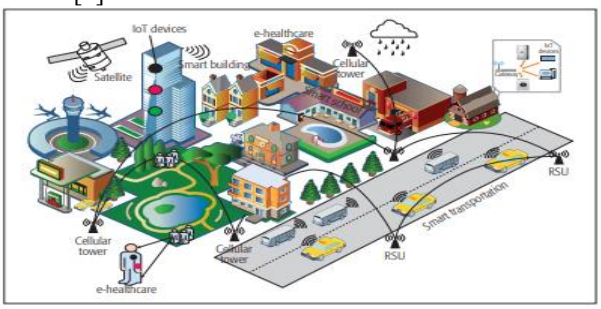

Figure 2 Smart City Architecture with IoT and Communication Networks

It is a city that is smart without being just this. It operates as a system, integrating citizens, local authorities, businesses, industries, and community groups. Its scope doesn't end with the boundaries of a city; it progresses further into regional governance and inter-municipal collaboration. High-tech development does a lot with respect to the IA, but one should not lose sight of his or her implications concerning people and institutions when using technologies. Above all, the very purpose of a smart city is to get all these into his value proposition [5], generating returns not only in the financial outcome but also in the quality of life, health, education, and time efficiency for every stakeholder.

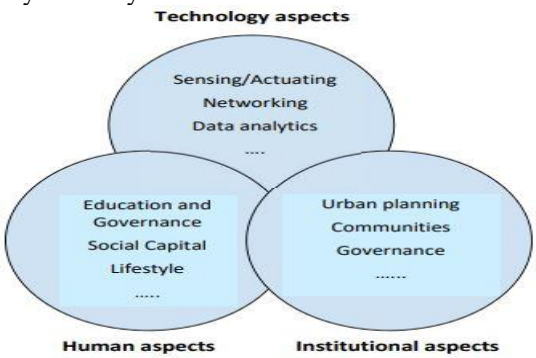

Figure 3 Interconnected Aspects of Smart

Smart cities can change lives by enabling items to converse and coordinate within the different and dispersed computing environments that will embody this vision of pervasive computing. This means delivering real-time information and services to the urban systems and citizens, something that is starting to change the way cities operate technologically. IoT, as a socially disruptive technology, is in the process of reshaping the complete techno-urban ecosystem and bringing innovations to many areas [6]. Specifically, IoT can enhance patient care by enabling remote monitoring, collecting, and analyzing data through interconnected devices and sensors in healthcare. Thus, IoT has an extensive outreach into smart healthcare in smart city architectures [7]. The ever-evolving nature of the Internet of Things (IoT) technology is now tending to make major changes in smart cities concerning effective data access, analysis, and automation across various sectors [8]. One of the key characteristics of IoT-based smart cities is real-time monitoring and control, where efficient real-time monitoring via central systems can keep track of critical parameters such as power use and health metrics, thus improving efficiency and safety in operations [9]. New generation infrastructure is also benefitting from advancements in practice, including precision agriculture applications that employ autonomous vehicles and sensors for monitoring variables such as soil moisture and crop health in even the most inaccessible locations [10]. Improved services to citizens have been extended, such as remote work and online education and e-commerce; however, these have made their way into the new security challenges of data privacy and security due to their accessibility to sensitive personal information [11]. Optimization of energy consumption using sensor-driven data will actually help in energy efficiency and sustainability in homes and pollution reduction and better management of the environment [12]. The privacy and public security would form the main issues in IoT systems particularly with the cross-domain authentication vulnerabilities. Currently, exploring the possible solutions to manage identities and access credentials securely across heterogeneous IoT networks are the applications of blockchain technology [13].

A. IoT System Architecture for Smart Cities

Cities all over the world today are being modernized into smart cities thanks to the wide-ranging and Information Communication Technology (ICT)-based implementation of advanced technologies like the Internet of Things (IoT) for the purpose of improving urban services, elevating quality of life, and stimulating sustainable developments [14]. Central in this transition is the architecture of IoT that is usually structured in terms of five interconnected layers which are the Sensing Layer, Network Layer, Middleware Layer, Gateway Layer, and Application Layer [15]. The functions within these layers include sensing, data collection that goes through transmission, processing, and user interface with the end-user. 5G in the Network Layer enhances connectivity and speed [16], while Application Layer intuitively designed user interfaces improve user satisfaction [17]. The Sensing Layer monitors the environmental and physiological data via sensors and WBANs, albeit with rising concern for data protection [18]. Middleware solutions will address issues regarding scalability, heterogeneity, and integration [19], wherein the Gateway Layer serves the purpose of effective transmission of data through LPWAN and Zigbee protocols [20]. Modular and scalable IoT architectures for smart cities are also critical for the efficient analysis of data and provision of services for sectors such as traffic control, energy consumption, and public safety. The systems enable data-based decision-making that supports urban planning, reduces expenses, and integrates inclusivity, sustainability, and adaptable technology [21].

Figure 4 Architecture of IoT Framework [15]

B. Technological Components of IoT Architecture

The pillar of a smart city, of course, is the Internet of Things. Advanced sensors, communication protocols, cloud and edge computing, and AI-powered analytics are used to bring intelligent urban living to realization [22]. The Internet of Things, which connects pervasive technologies like Wi-Fi, 4G-LTE, and the emerging 5G networks, makes real-time data capture possible and service operation ubiquitous. Major components of IoT include sensing devices, messaging protocols, i.e., MQTT, CoAP, AMQP, HTTP, and scalable, low-latency cloud computing and edge computing [24]. AI and machine learning improve smart-cite functions, but they require appropriate regulations for ethical use. IoT results operational efficiencies into manufacturing, citizen engagement, and sustainability [25]. The role of several barriers to the adoption of IoT includes security, integration, high costs, and data management issues. The effects of IoT span intelligent transport systems, energy-efficient buildings, waste management, and public safety in optimizing urban services [27-29]. For example, smart street lighting, using networks of sensors and controllers, is much more energy efficient and waste less than conventional systems [31].

II.LITERATURE REVIEW

In order to fulfill the United Nations Sustainable Development Goals (UNSDG) 11: Sustainable Cities and Communities, **Zeng, F., Pang, C., & Tang, H. (2024) [33]** outlined how the Internet of Things (IoT) is an essential part of smart cities. Critical elements of smart cities, including data collection, creation, processing, analysis, and application handling, are provided by the Internet of Things (IoT), an infrastructure that allows objects to connect with one another via the Internet. Applications built on the Internet of Things can support sustainable urban growth. Numerous studies have shown how the IoT may enhance the sustainable development of smart cities. With an emphasis on the implications for sustainable urban development, this systematic study offers insightful information about the use of the Internet of Things in smart city settings. We explore how IoT contributes to the sustainable growth of smart cities by examining 73 articles, with particular attention to smart communities, smart transportation, disaster relief, privacy and security, and new applications. We have described the characteristics of IoT sensors in depth for each domain. Furthermore, we have looked at a number of protocols and communication technologies that are appropriate for sending data generated by sensors. Additionally, we have provided the techniques for integrating and analysing this data at the IoT application layer. Lastly, we point out areas in the literature that need more research by identifying the present study.

Within the METACITIES program, **Faliagka, E., et al. (2024) [34]** offered a novel solution to the problems of smart mobility by utilizing digital twins. The growing complexity of urban transportation networks and the pressing need to increase city sustainability, safety, and efficiency are the reasons we have been working on this topic. This paper's work is a component of the METACITIES initiative, an Excellence Hub that covers a wide geographic area—that is, Southeastern Europe. In order to enable real-time monitoring, analysis, and decision-making, the Greek innovation ecosystem METACITIES uses digital twin technology to build intelligent duplicates of urban transportation environments. We illustrate how digital twins can improve traffic flow, reduce environmental impact, and improve emergency response through use cases like "Smart Parking," "Environmental Behavior Evaluation on Traffic Incidents," and "Emergency Management." These scenarios will be tested on a small scale before a larger and more costly scale implementation is decided upon. The METACITIES Architecture for smart mobility is the end result, and it will be a component of an Open Digital Twin Framework that may transform a smart city into a metacity.

According to **Syed, A. S., et al. (2021) [35],** the Internet of Things (IoT) is a system that eliminates the need for human interaction by integrating various devices and technology. This makes it possible for cities all over the world to become smarter. The internet of things has led the creation of smart city systems for sustainable living, enhancing citizen comfort and productivity by hosting various technologies and enabling interactions between them. The Internet of Things for Smart Cities operates across a wide range of disciplines and rely on a number of underlying systems. We present a comprehensive analysis of the Internet of Things in smart cities in this study. The basic elements of the IoT-based Smart City landscape are covered first, then the technologies that make these domains possible, including the architectures and networking technologies used, as well as the artificial algorithms implemented in IoT-based Smart City systems. A survey of the most widely used procedures and apps across different Smart City domains is next. The last section discusses the difficulties in deploying IoT systems for smart cities and how to overcome them.

The addition of Internet of Things (IoT) networks into intelligent cities is essential to improving the effectiveness of municipal operations and services, according to **Tekinerdogan, B., Köksal, Ö., & Çelik, T. (2023) [36].** It is crucial to design a smart city architecture that can change to meet the ever-evolving functional and qualitative requirements of city services. But during this process, important choices have to be made about communication protocols, security and safety, time performance, and data processing capability. This study suggests a methodical way to direct the system architecture design of IoT-based smart cities in order to address these issues. Selected

architectural viewpoints are used to model the design while taking important stakeholders' concerns into account. This study also offers insightful information on the difficulties and lessons discovered when developing IoT-based smart cities. Future study in this area can be facilitated by this information, which can also help practitioners create such smart cities. Smart city architects can create a reliable and flexible system architecture that can satisfy the changing demands of smart city services by using the suggested methodology.

As **Jiang (2020) [37]** states, the rapid growth and extensive application of the Internet of Things (IoT) and cloud computing have increasingly formed a "smart" modern society, which has extended to smart cities. The conventional urban systems, which have been inefficient and isolated, have not been able to exchange information in an effective way. This study investigates the development of IoT, cloud computing, and smart cities, emphasizing their technologies, structure, and application. Jiang comes up with an IoT-enabled and cloud-based intelligent city system to study transmission networks, sensors, system design, and application platforms. The work solves the communication failure problem among IoT sensor networks by proposing an approach of using Markov chains for data aggregation to enhance the transfer of information and facilitate correct retransmission of data so that the problem of information islands is avoided, and effective exchange of information occurs between different subsystems.

As per **Janani, R. P., et al. (2021) [38],** smart cities are a significant field that is currently achieving remarkable heights. The Internet of Things is crucial to the development of smart cities. People in the nation with smart cities will be highly developed socially and economically, and their level of knowledge and quality of life will also significantly improve. The introduction of smart cities will decrease the amount of time and human effort required to complete tasks by hand. The ecology of a smart city can shield its citizens from natural disasters, tragedies, and challenging circumstances. By all means, the development of smart cities will save time waste in our daily lives. This study primarily explains what a smart city is, how it is developed, its applications, problems, real-time applications, potential future developments, etc. There is also discussion of the IoT technology and the gadgets that are utilized to construct smart cities.

The "smart city" as proposed by **Ghazal et al. (2021) [39]** describes a set of ideas and technological solutions intended to make cities more efficient, sustainable, and inclusive. Emerging as a phenomenon of the 2000s, it aims at solving urban challenges like shortages in resources, health, demographic transitions, and pollution, making optimal use of digital technologies. Smart city involves not only technological advances but also non-technical progresses that contribute towards urban sustainability. One of the most promising fields for smart cities is the application of IoT-based sensor networks in healthcare, which, when combined with machine learning, can manage large volumes of data efficiently. This research is a benchmark for future studies on the role of IoT in healthcare in smart cities.

According to **Mirani (2022) [40],** remote monitoring, intelligent analytics, and control of industrial processes are all tools through which IoT drives evolution. However, with respect to industrial development solutions, full-stack establishment with IoT is nascent, and challenges impede its adoption. Various IoT architectures have been proposed by researchers, based on different layers and technologies, for the end-to-end integration of IoT systems. This paper reviewed and compared three widely accepted IoT reference architectures, presenting a state-of-the-art review of the conceptual and experimental IoT architectures from the literature. The study identified the main architectural requirements for IoT to be scalability, interoperability, security, privacy, reliability, and low latency and determined how current architectures offer solutions to these requirements using, for instance, emerging technologies of edge/fog computing, blockchain, software-defined networking (SDN), 5G, machine learning, and wireless sensor networks (WSN). The study further discussed the relationship of current challenges and emerging technologies, including opportunities and future research directions.

Domínguez-Bolaño (2022) [41] explained on the growing requirement of the IoT platforms for housing the incredible variety of devices which might be manufactured by several producers with the utilization of totally different protocols and data formats and their communications technologies. This article elaborately reviewed the prevalent architectures, technologies, protocols, and data formats from existing IoT platforms. The author desired to demonstrate the laborious management problem regarding heterogeneous devices and communication among different IoT ecosystems through that study. In addition, a very comprehensive comparative evaluation of open-source IoT platforms, analysing them according to several significant characteristics like scalability, flexibility, interoperability, or security, has been carried out through this research work. This thorough comparison is supposed to help organizations select the most appropriate IoT platform according to their specific requirements for using it to manage and control them in heterogeneous and multi-vendor environments.

III.OBJECTIVES

- Develop a robust deep learning system for classifying vehicle behaviour in transportation systems, detecting various attack types like DoS, Whitewash, and Brute Force using advanced machine learning techniques.
- Integrate Neural Networks (NN), XGBoost, and Logistic Regression to enhance attack detection accuracy, while leveraging an Attention mechanism to prioritize significant patterns in the transportation data.
- Address class imbalance in the dataset using the SMOTE algorithm, ensuring fair representation of all attack types, and improving the model’s ability to classify underrepresented attacks effectively.

- Evaluate the model using key performance metrics such as Accuracy, Precision, Recall, F1-Score, and ROC-AUC, ensuring reliable real-time attack detection for continuous monitoring of transportation systems.

IV.METHODOLOGY

The transportation system security is the focus of the project, which aims to detect and classify various attack types such as DoS, Whitewash, and Brute force by advanced deep learning techniques based on the vehicle behaviour. The hybrid Neural Network (NN) model is fed by SMOTE to counter imbalanced data; other classifiers such as XGBoost and Logistic Regression help enhance robustness. It uses features like trust_degree, time, and location to detect malicious behaviour patterns. The NN model is augmented with Gaussian Noise and Batch Normalization, while training is conducted with EarlyStopping and ReduceLROnPlateau, thus avoiding overfitting. This ensures high attack integrity and early detection in transportation systems. A rigorous monitoring and classifying system on attacks like Denial of Service, Whitewash, and Brute Force attacks, identifying issues of class imbalance and variability, is intended in developing such a system through transportation data. Within the approach of deep learning, it aims to include broad NN features for feature extraction that can handle important features such as trust degree, hour, day of-week, and location so that both static and dynamic aspects of vehicle behaviour can be modelled. Focal Loss improve on classification of those difficult-to-classify samples while class imbalance can be solved using SMOTE (Synthetic Minority Over-sampling Technique). The SD-MTC thus resulted in a reliable and scalable system that could potentially offer real-time attack detection with fewer false positives in order to further boost the quality of decision making in transportation security and, hence, open the way for further developments into advanced monitoring and security applications.

The study employed Python and various libraries, such as NumPy, Pandas, Matplotlib, and Seaborn, to create a vegetation system for identifying attack types in transportation systems. Classification was done using XGBoost, while TensorFlow-Keras created and trained the Neural Network (NN) model. Scikit-learn assisted in pre-processing, model validation, and evaluation metrics, while SMOTE handled class imbalance. The system was run on Google Colab, supporting their use of GPU acceleration and integrated libraries. A hybrid system involving NN for feature extraction, XGBoost for sequential learning, Logistic Regression for baseline classification, and Attention for improvement in accuracy was developed. Data augmentation techniques such as Jittering, Scaling, and Time-Warping enhanced robustness, while SMOTE synthesized extra samples to deal with class imbalance. This hybrid system allows for scalable, real-time attack detection, increasing the safety of transportation systems.

A. Usage of machine learning methods for earlier detection

Previous studies in smart transport systems have on one hand undertaken efforts to improve data quality and classification accuracy for the detection of suspected malicious activities. One common method for balancing datasets and improving model performance is the Synthetic Minority Over-sampling Technique (SMOTE), which is applied to tackle the problem of class imbalance by making sure that the minority class examples are well represented in training data. In this project, SMOTE was applied to balance the non-malicious and the malicious behaviour data in order to strengthen the model's ability to perform anomaly detection. After the application of SMOTE, feature extraction, and computation of degree of trust in the data were used for assessing data validity with degree of trust being calculated with respect to experience, performance, and behaviour. The degree of trust was then used to classify the different attack types including DoS, Whitewash, Brute force, and non-malicious behaviour, rather than on old signal processing methods. Performance assessment of the model was done using metrics such as accuracy, precision, recall, F1 score, and ROC-AUC to check how well it discriminates between malicious and non-malicious data. Visualization tools such as confusion matrices, ROC curves, and precision-recall plots helped showcase how effective the attack detection pipeline was, which were aligned with the security objectives of smart transport systems.

B. Proposed Model

This study developed a hybrid machine learning model aiming to enhance the classification and detection of attack types on transportation systems. The model consists of Neuro Networks for feature extraction, XGBoost for sequential learning, and Logistic Regression for solid classification, including an Attention mechanism focusing on the most important patterns of data.

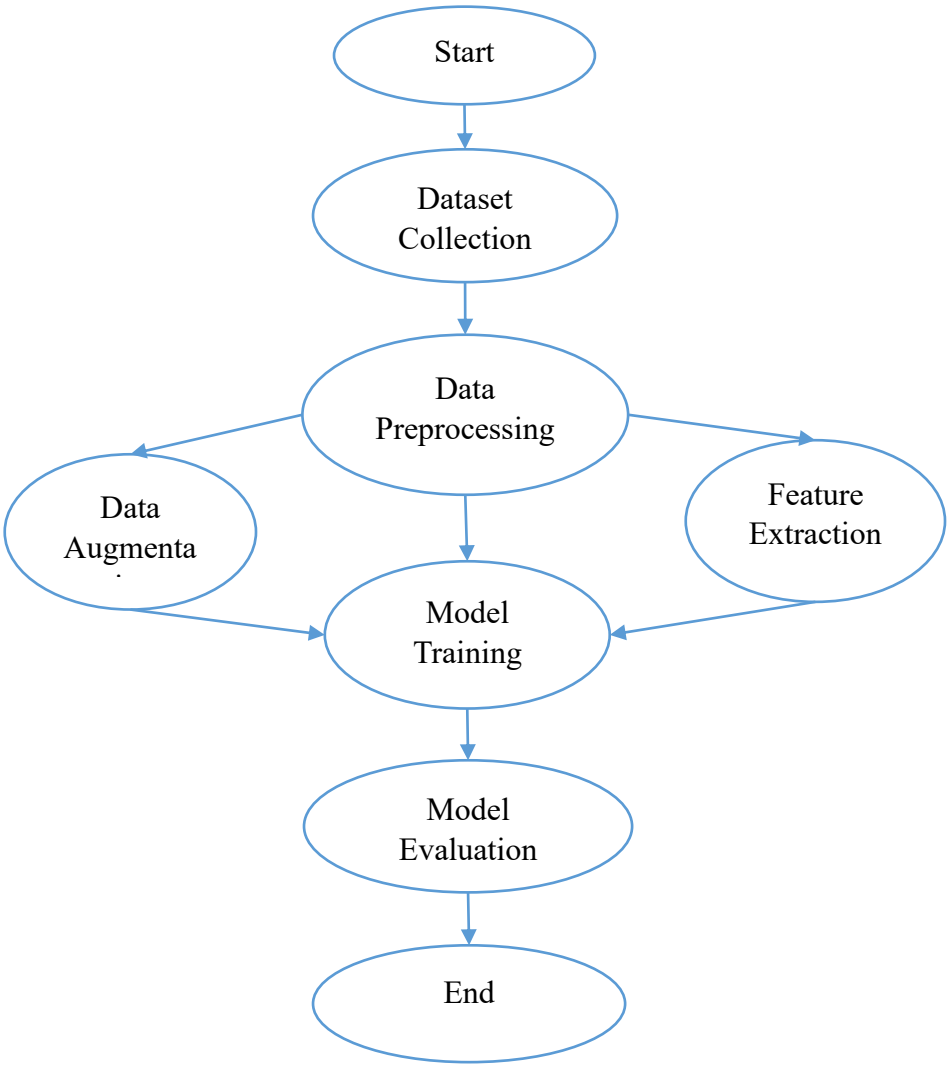

Figure 5 Flow Chart of Methodology

The NN brings in spatial aspects such as trust_degree, location, and time-based variables; while XGBoost takes care of the temporal aspect, identifying long-term patterns of vehicle behavior. Logistic Regression acts as a baseline classifier while the Attention mechanism emphasizes the focal data points, assisting the subtle detection of malicious activities like Denial of Service (DoS), Whitewash, and Brute Force attacks. The methodology was carried out through various steps to ensure ideal performance of the model. The main data pre-processing tasks comprised cleaning, normalizing the transportation data, segmentation into sliding windows, and fixing missing values due to resampling and imputation. Other important steps were the extraction of key features such as trust_degree and location dynamics, which were later subjected to augmenting techniques like jitter, scaling, and time-warping for better robustness of the model. And to counter class imbalance affecting the poorer attack types, SMOTE was introduced to create synthetic samples. Thus, the hybrid model training, enhanced with Focal Loss to place greater emphasis on the harder-to-classify samples, increased the overall model precision and accuracy. For evaluation, levels of precision, recall, F1, accuracy, and ROC-AUC curves were employed, alongside confusion matrixes and time-series plots, in order to visualize the model efficiency in detecting types of attacks and perform in real-time.

C. Hybrid Model

The study developed a hybrid machine learning model combining Neural Networks (NN), XGBoost, and an Attention mechanism to detect and classify attack types in transportation systems. In this, the NN was used first to extract spatial features from transportation-related data including critical parameters of trust degree, vehicle location, and time of day to identify patterns showing malicious behaviors such as DoS attacks or Whitewash attacks. After this, NNs were able to process the data spanning several layers with activation functions, foremost being ReLU, learning complex, non-linear relationships with the data setting an initial path for an effective attack classifier. Subsequently, with spatial features extracted via NN, the temporal analysis was performed by XGBoost in order to capture sequential dependencies in vehicle behavior over time-XGBoost shines in capturing the gradual nature of attacks like the gradual shift in vehicle behavior generally attributed to Brute Force and Whitewash

attacks. XGBoost employs decision trees that allow for the efficient handling of large datasets, thereby assigning different degrees of importance to temporal features and allowing pattern extraction across intervals of time. Finally, the integration of both NN and XGBoost and Attention, further refined model focus by weighting the more relevant portions of the data like sudden shifts in trust degree or location. The mechanism of Attention allowed the model to focus on key points that best represented attack activity, thereby enhancing the sensitivity and precision of the system. This hybrid model that integrated both spatial and temporal learning with selective attention was very efficient to detect a variety of attack types in real time, thus providing solid and uninterrupted monitoring of vehicle behavior in transportation systems. By leveraging all properties of the NN, XGBoost, and Attention, the system becomes a scalable solution to detect DoS, Whitewash, Brute Force, and other kinds of malicious behavior, assuring timely detection and response to security threats.

D. Evaluation Metrics

The performance of attack detection model based on NN + XGBoost + Attention hybrid model for Transportation System was evaluated on some key performance metrics as follows:The measure of accuracy refers to how well overall the system is performing; that is, it shows the ratio between cases which are classified correctly - malicious or otherwise. It is calculated as -

$$\text{Accuracy} = \frac{\text{True positive} + \text{True Negetive}}{\text{TotalNumber of Instance}}$$

Of course, accuracy must be interpreted along with other metrics, particularly within imbalanced datasets, although it is desirable for high accuracy. The ratio evaluates the skill of the model in precisely identifying incorrect malicious behaviour while also failing to classify good behaviour as malicious. Precision can be calculated as:

$$Precision = \frac{True\ positive}{True\ Positive + False\ Positives}$$

High precision means few false positives, which creates a smooth operating environment for systems. Recall (sensitivity) indicates how well malicious cases can be detected from their actual occurrence. It is calculated as:

$$\text{Recall} = \frac{True\ Positives}{True\ Positives + False\ Negatives}$$

The higher the recall, the better chances of early detection of attacks and identifying their malicious behaviours even before they affect system security. It is a symmetric average between precision and recall; thus, the F1-Score is especially relevant when making a trade-off between false positives and false negatives. Its exact mathematical formulation is given below:

$$F1 - Score = 2 \times \frac{Precision\ \times Recall}{Precision + Recall}$$

A big F1-Score indicates good detection performance with a low false alarm rate. The main aim of the confusion matrix is to visually describe the set of true positives, true negatives, false positives, and false negatives so that one might see functional areas to improve the classification process. The ROC-AUC assesses the model's ability to discriminate between classes by plotting the True Positive Rate against the False Positive Rate at various threshold settings. A greater AUC (closer to 1) means better performance. An expensive ROC-AUC value shows the model can effectively distinguish between malicious and nonmalicious behaviours.

V.RESULTS AND DISCUSSIONS

It presents the evaluation performance of hybrid machine learning models that are Neuro Networks (NN), XGBoost and the Attentive mechanism for attack detection in transportation systems. In the model, NN extracts the spatial features like the key pattern's degree of trusts by variations and location shifts whereas XGBoost detect temporal dependencies analyzing dynamic behavior of vehicles and evolving attacks through it. Attention will be for finetuning the value that the model lays on bits of critical information to improve the accuracy with which its detection will be for relatively subtle types of attacks such as Denial of Service. The evaluation metrics that provide a complete assessment of the model capability towards the detection or misbehaviors are Accuracy, Precision, Recall, F1-Score, Confusion Matrix and ROC-AUC. The performance of the model is further tuned using SMOTE class balancing, early stopping, and learning rate changes. This kind of hybrid approaches lets the systems function as very reliable real-time attack detection as well as monitoring in transportation systems, which could later be increased with added regression metrics.

A. Hybrid Machine Learning Approach for Attack Detection in Transportation Systems with Behaviour Anomaly Visualization

The study undertaken concerning security and anomaly detection in smart transport systems has primarily revolved around issues such as enhancing data quality, balancing datasets, and the evaluation of performance metrics in an attack classification context. It describes the process of extracting transportation system data, pre-processing them, for example, imputing them through Simple Imputer for missing values, and performing SMOTE on the data to achieve class balance. It should also assure that the dataset appropriately includes malicious and non-malicious behaviors. The trust degree is assigned based on experience, performance, and behavior, and will be used as a basis for classifying different attack types, such as DoS, Whitewash, Brute Force, and the rest for including non-malicious behavior. Model evaluative metrics entail Accuracy, Precision, Recall, F1-Score, and ROC-AUC, all indicating the ability of the model to detect and classify attacks. Attainment of these key metrics includes Accuracy (91.53%), Precision (1.0000), Recall (0.8462), F1-Score (0.9167), and ROC-AUC (1.0000). The Precision score of 1.0000 shows there weren't any false positives. Recall indicates that 84.62% of malicious instances have been

identified. The F1-Score gives an equally weighted view of performance, while the perfect ROC-AUC score substantiates the model's ability to differentiate between malicious and non-malicious instances. All this evaluation combines to show the efficiency of the model in real-time attack detection for ensuring economic transportation system security.

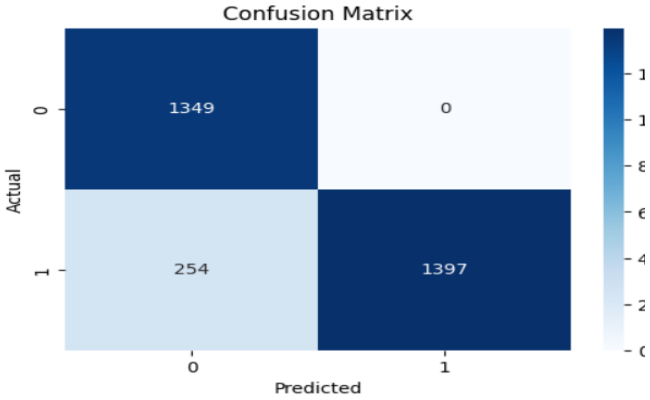

Figure 6 Confusion Matrix

The confusion matrix in Figure 6 shows the model classification results, whereby it correctly classified 1349 instances as Non- Malicious (True Negatives) and 1397 instances as Malicious (True Positives). It also shows that 254 instances were classified as non-malicious when in fact they were malicious (False Negatives) while there were no false positives. These values give an overview of the model classification performance. Table 1 also depicts the distribution of attack types in the dataset: Non-Malicious (1600 instances), being the dominating type of behavior that has correctly been identified as non-malicious behaviour by the dataset. Attacks Due to DoS manner were huge in number, that is, 1349 instances, and Brute Force attacks were the rare ones (33 instances), and Whitewash attacks were the rarest with only 18 instances being detected.

Table 1 Attack Detection Results

Attack Type	Count
Non-Malicious	1600
DoS	1349
Brute Force	33
Whitewash	18

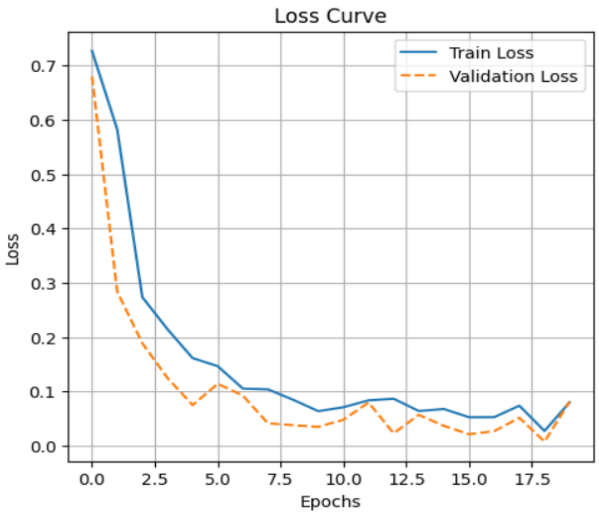

Figure 7 Loss Curve

Several curves visualize the model's performance, such as the loss curve. The train loss is sharply declining in the loss curve of Figure 7, which indicates that the model is learning; on the other hand, the validation loss fluctuates toward the later epochs-in other words, pointing to overfitting. The two curves level off, implying that convergence is close. In Figure 8, the curve for accuracy indicates that the train accuracy first increases, while we observe validation accuracy at higher values, fluctuating, thus showing some sign of overfitting. Even as train accuracy approaches 1.0 due to strong learning, validation accuracy seems to stabilize with a few variances. The F1-Score against Decision Threshold curve in Figure 8 proves that at low decision thresholds, the F1-Score is high with the trade-off on sensitivity by the model but falls as the decision threshold goes higher, thereby indicating more of a trade-off between sensitivity and precision. All the graphs taken together will signify that the model is performing considerably well but needs to be improved since overfitting needs to be reduced and fine-tuning for decision threshold is to be drawn closer to perfectly classifying balance.

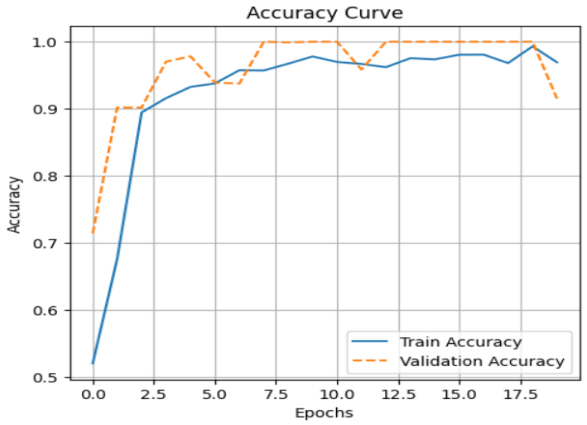

Figure 8 Accuracy Curve

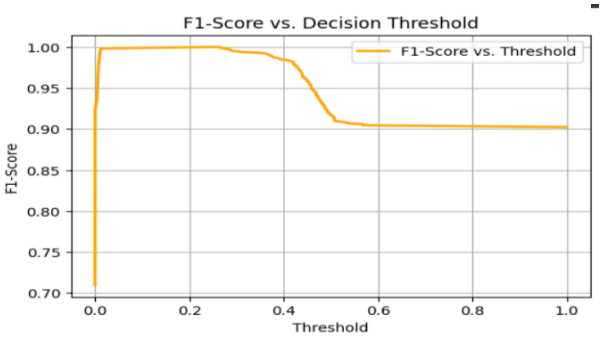

Figure 9 F1-Score vs. Decision Threshold

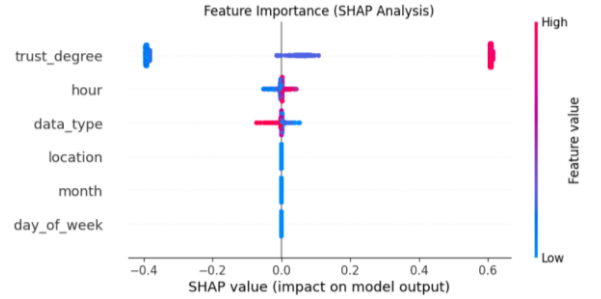

Figure 10 Feature Importance (SHAP Analysis)

As shown in Figure 10, the Feature Importance (SHAP analysis) plot outlines the significance of various features toward the model output. Trust Degree is noted to be the most important feature; it has an extensive range of SHAP value distributions pointing toward its importance in the model's prediction. Hour affects the prediction quite a bit; Data Type, Location, Month, and Day have lower contributions with SHAP values clustered around zero. The colour scale (blue to red), which represents the range of the feature value, shows the influence each feature's value has on the model. This plot shows which features the model relied on the most for prediction.

B. Merging NN, XGBoost, and Logistic Regression Predictions Using Attention Mechanism for Attack Detection in Transportation Systems

After training Neural Network (NN) and XGBoost models, the second layer of merging is achieved by an Attention mechanism for better accuracy and reliability in attacks detection in transportation systems. The NN extracts spatial patterns, highlighting features like trust degree, vehicle location changes, and time-based anomalies, while XGBoost handles temporal dependencies and analyses the change in vehicle behaviour over time. On the other hand, the hybridization allows for both spatial and temporal aspects to be considered, which are critical in detecting attacks such as denial of service (DoS), whitewash, and brute-force attacks. The Attention mechanism dynamically weights which time steps are most relevant based on their contribution to the changes in data, such as sudden drops in trust or location transitions. This in turn improves delicacy by reducing noise in the model. This hybrid approach, combining NN for feature extraction, XGBoost for temporal learning, and Attention for selective enhancement, results in stable, accurate, and interpretable predictions, hence, the model gets the desired properties of being efficient for a real-time attack detection system and monitoring vehicle behaviour continuously in transportation systems.

C. Final Evaluation and Performance Metrics

The performance of the model is evaluated with key metrics like Accuracy, Precision, Recall, F1-Score, Confusion Matrix, ROC-AUC, etc., to analyze the model's capability of differentiating between non-malicious and malicious behavior of DoS, Whitewash, and Brute Force attacks. Accuracy gives a general performance assessment, Precision low false positives, and Recall minimizing false negatives, which are very critical in real-time detection. The F1-Score balances both scores, especially in asymmetric datasets, and Confusion Matrix helps in recognizing misclassifications. In the case of ROC-AUC, it shows the differentiation capability of the model in attack types; few features like trust degree and location changes validate the model's comprehension of vehicle behavior. Such metrics provide a good insight into the model's strengths and lead to further improvements for much more accurate, real-time detection of attacks in transportation systems.

Table 2 Hybrid Model Performance Metrics

Metric	Score
Accuracy	0.9737
Precision	1
Recall	0.9522
F1-Score	0.9755
ROC-AUC	0.9999

The performance metrics in Table 2 show that the model has very good classification abilities. It has an Accuracy of 97.37%, indicating that it could predict almost every single instance correctly. The Precision was perfect (1.0000), meaning that there were absolutely no false positive errors; in addition, Recall was relatively high at 95.22%, meaning that most Malicious instances were detected. The F1-Score of 0.9755 indicates a near-equal balance between precision and recall, minimizing false positives and false negatives. The ROC-AUC score of 0.9999 indicates near-perfect discriminatory ability of the model for the Malicious and Non-Malicious instances with very few errors showing the strength of the model performance in real-time attack detection.

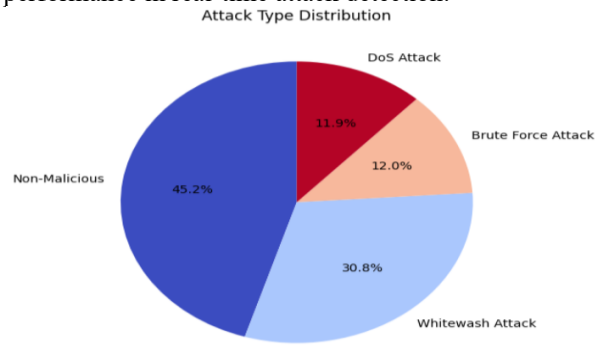

Figure 11 Attack Type Distribution in Percentage

Table 3 Distribution of Detected Attack Types

Attack Type	Count
Non-Malicious	1357
Whitewash Attack	925
Brute Force Attack	361
DoS Attack	357

As shown in Table 3, the distribution of detected attack types is as follows: Non-Malicious behavior is detected the most, with 1357 instances, demonstrating that the system is able to tell the useful from the irrelevant. Whitewash attacks come next with 925 instances, implying that the system can detect attempts at persuasion of data on the basis of corrupt intention. The system detects Brute Force attacks 361 times, showing its ability to recognize multiple unwanted attempts at access occurred using the same method, while DoS attacks resorted to by the attackers amount to 357 instances, displaying the system's capability of detecting attempts to disrupt or overload the service.

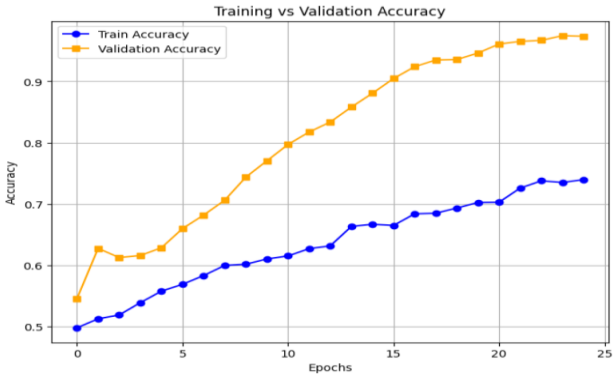

Figure 12 Training vs Validation Accuracy

The Training vs Validation Accuracy plot in Figure 12 depicts the evolution of model accuracy through training. The blue line is for training accuracy, while the orange line is for validation accuracy. Training accuracy starts relatively low, but increases consistently, indicating the model is learning the training data; past the first half of training, the validation accuracy reaches higher levels faster, indicating good generalization to the validation set. This is a common and healthy sign that both have come together in the later epochs with appropriate learning. Some separation is maintained between the two curves, which indicate no overfitting, as both curves continue rising smoothly.

VI. Conclusion

This study has successfully created a hybrid machine learning model bringing together Neural Networks (NN), XGBoost and Attention to boost detection and classification of such malicious behaviors in transportation systems. It relies on high-performing deep learning techniques to assess attacks flipping formats like DoS, Whitewash and Brute Force through vehicle behavior data. Important key performance parameters, which include such terms as Accuracy, Precision, Recall, F1-Score, and ROC-AUC, show that there is an exceptional capacity of the model to differentiate between malicious and non-malicious behaviors and has thus highly reliable potential in real-time attack detection. Integration between SMOTE for class balance and Attention focusing on crucial data points increased the effectiveness of the model while it also reduces false positives and provides timely identification of threats in trying times. It offers an evaluation framework that establishes a scalable, reliable, and viable solution in such areas like the security and monitoring of transportation systems with a promising outlook for future developments in smart city applications.

Conflict of Interest: The corresponding author, on behalf of second author, confirms that there are no conflicts of interest to disclose.

Reference

[1] Padhiary, M., Roy, P., & Roy, D. (2025). The Future of Urban Connectivity: AI and IoT in Smart Cities. In *Sustainable Smart Cities and the Future of Urban Development* (pp. 33-66). IGI Global Scientific.

[2] Rajab, H., & Cinkelr, T. (2018, June). IoT based smart cities. In *2018 international symposium on networks, computers and communications (ISNCC)* (pp. 1-4). IEEE.Zangaraki, S., Mirabi, M., Erfani, S. H., & Sahafi, A. (2025). SecShield: An IoT access control framework with edge caching using software defined network. *Peer-to-Peer Networking and Applications*, *18*(1), 1-17.

[3] Radzuan, S. A. M., Brahim, J., Nguyen, Q., & Ponniah, V. CURRENT PRACTICES OF INTERNET OF THINGS (IoT): THE DEFINITION AND ITS INTEGRATION WITHIN JOINT VENTURES (JV) COMPANY IN MALAYSIAN CONSTRUCTION INDUSTRY. *MALAYSIAN CONSTRUCTION RESEARCH JOURNAL (MCRJ)*, 325.

[4] Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., & Guizani, S. (2017). Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Communications Magazine*, *55*(9), 16-24.Shahrour, I., & Xie, X. (2021).

[5] Lea, R. (2017). Smart cities: An overview of the technology trends driving smart cities. *IEEE Advancing technology for Humanity*, *3*(March), 1-16.

[6] Bibri, S. E. (2018). The IoT for smart sustainable cities of the future: An analytical framework for sensor-based big data applications for

environmental sustainability. *Sustainable cities and society*, *38*, 230-253..

[7] Abdulmalek, S., Nasir, A., Jabbar, W. A., Almuhaya, M. A., Bairagi, A. K., Khan, M. A. M., & Kee, S. H. (2022, October). IoT-based healthcare-monitoring system towards improving quality of life: A review. In *Healthcare* (Vol. 10, No. 10, p. 1993). MDPI.

[8] Ejaz, U., Ramon, W., & Jeol, P. (2025). IoT for Hazard Detection and Worker Safety Monitoring.

[9] ur Rehman, A., Alblushi, I. G. M., Zia, M. F., Khalid, H. M., Inayat, U., Benbouzid, M., ... & Hussain, G. A. (2025).

[10] Padhiary, M. (2025). The Convergence of Deep Learning, IoT, Sensors, and Farm Machinery in Agriculture. In *Designing Sustainable Internet of Things Solutions for Smart Industries* (pp. 109-142). IGI Global.

[11] Huang, X. (2025). The Dilemma And Solution Of Citizen Privacy Protection In The Governance Of Network Social Security.

[12] Naz, L. F., Qamar, R., Asif, R., Hina, S., Imran, M., & Ahmed, S. (2025). Intelligent energy management in IoT-enabled smart homes: Anomaly detection and consumption prediction for energy-efficient usage. *Mehran University Research Journal of Engineering and Technology*, *44*(1), 113-123.

[13] Ma, X., Fang, F., & Wang, X. (2025). Dynamic Authentication and Granularized Authorization with a Cross-Domain Zero Trust Architecture for Federated Learning in Large-Scale IoT Networks. *arXiv preprint arXiv:2501.03601*.

[14] Omrany, H., Al-Obaidi, K. M., Hossain, M., Alduais, N. A., Al-Duais, H. S., & Ghaffarianhoseini, A. (2024). IoT-enabled smart cities: a hybrid systematic analysis of key research areas, challenges, and recommendations for future direction. *Discover Cities*, *1*(1), 2.

[15] Sahu, S. K., & Mazumdar, K. (2024). Exploring security threats and solutions Techniques for Internet of Things (IoT): from vulnerabilities to vigilance. *Frontiers in Artificial Intelligence*, *7*, 1397480.

[16] Marrone, P. (2024). *Exploring Device-to-Device (D2D) Communication in Cellular Technology: 5G and Beyond* (Doctoral dissertation, Politecnico di Torino).

[17] Dharmawan, D., Febrian, W. D., Karyadi, S., & Sani, I. (2024). Application of Heuristic Evaluation Method to Evaluate User Experience and User Interface of Personnel Management Information Systems to Improve Employee Performance. *Jurnal Informasi Dan Teknologi*, 14-20.

[18] Gurusamy, V., Praveenkumar, P., Jebaraj, J. R., Ranjithi, M., & Raphael, B. L. (2024, March). A lightweight multi-layer authentication protocol for wireless sensor networks in IoT applications. In *AIP Conference Proceedings* (Vol. 2966, No. 1). AIP Publishing.

[19] Singh, A. K., & Bhola, A. (2024). IoT-enabled Data Acquisition in Urban Landscapes. *Available at SSRN 4742000*.

[20] Pranavasri, V. J. S. (2024). *Towards Scalable Architectures in oneM2M-based Interoperability deployments in Smart Cities* (Doctoral dissertation, International Institute of Information Technology, Hyderabad).

[21] Zaman, M., Puryear, N., Abdelwahed, S., & Zohrabi, N. (2024). A Review of IoT-Based Smart City Development and Management. *Smart Cities*, *7*(3), 1462-1500.

[22] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

[23] Sehrawat, D., & Gill, N. S. (2019, April). Smart sensors: Analysis of different types of IoT sensors. In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 523-528). IEEE.

[24] Naik, G. P., & Bapat, A. U. (2020). A brief comparative analysis on application layer protocols of internet of things: MQTT, CoAP, AMQP and HTTP. *Int. J. Comput. Sci. Mob. Comput*, *9*(9), 135-141.

[25] El-Sayed, H., Sankar, S., Prasad, M., Puthal, D., Gupta, A., Mohanty, M., & Lin, C. T. (2017). Edge of things: The big picture on the integration of edge, IoT and the cloud in a distributed computing environment. *ieee access*, *6*, 1706-1717.

[26] Ullah, Z., Al-Turjman, F., Mostarda, L., & Gagliardi, R. (2020). Applications of artificial intelligence and machine learning in smart cities. *Computer Communications*, *154*, 313-323.

[27] Lee, K., Romzi, P., Hanaysha, J., Alzoubi, H., & Alshurideh, M. (2022). Investigating the impact of benefits and challenges of IOT adoption on supply chain performance and organizational performance: An empirical study in Malaysia. *Uncertain Supply Chain Management*, *10*(2), 537-550.

[28] Papel, M. S. I., Mridha, A. A., Rahman, A., & Ashrafuzzaman, M. (2024). Enhancing Government It Infrastructure: Develop Frameworks For Modernizing Government It Systems To Improve Security, Efficiency, And Citizen Engagement. *Frontiers in Applied Engineering and Technology*, *1*(01), 157-174.

[29] Han, X., Dang, P., Liao, L., Song, F., Zhang, M., Zhang, M., ... & Siddique, K. H. (2025). Combining slow-release fertilizer and plastic film mulching reduced the carbon footprint and enhanced maize yield on the Loess Plateau. *Journal of Environmental Sciences*, *147*, 359-369.

[30] Ejaz, U., Ramon, W., & Jeol, P. (2025). Improving Equipment Utilization with IoT Sensors.

[31] Padhiary, M., Roy, P., & Roy, D. (2025). The Future of Urban Connectivity: AI and IoT in Smart Cities. In *Sustainable Smart Cities and the Future of Urban Development* (pp. 33-66). IGI Global Scientific Publishing.

[32] Sukumar, P., Jayasurya, S., Rohith, M., Premnath, E. S., Sugumar, K., & Mythily, V. (2025). IoT-powered street light management: Enhancing fault detection and reporting. In *Challenges in Information, Communication and Computing Technology* (pp. 136-140). CRC Press.

[33] Zeng, F., Pang, C., & Tang, H. (2024). Sensors on internet of things systems for the sustainable development of smart cities: a systematic literature review. *Sensors*, *24*(7), 2074.

[34] Faliagka, E., Christopoulou, E., Ringas, D., Politi, T., Kostis, N., Leonardos, D., ... & Voros, N. (2024). Trends in digital twin framework architectures for smart cities: A case study in smart mobility. *Sensors*, *24*(5), 1665

[35] Syed, A. S., Sierra-Sosa, D., Kumar, A., & Elmaghraby, A. (2021). IoT in smart cities: A survey of technologies, practices and challenges. *Smart Cities*, *4*(2), 429-475.

[36] Tekinerdogan, B., Köksal, Ö., & Çelik, T. (2023). System architecture design of IoT-based smart cities. *Applied Sciences*, *13*(7), 4173.

[37] Jiang, D. (2020). The construction of smart city information system based on the Internet of Things and cloud computing. *Computer Communications*, *150*, 158-166.

[38] Janani, R. P., Renuka, K., Aruna, A., & Lakshmi Narayanan, K. (2021). IoT in smart cities: A contemporary survey. *Global Transitions Proceedings*, *2*(2), 187-193.

[39] Ghazal, T. M., Hasan, M. K., Alshurideh, M. T., Alzoubi, H. M., Ahmad, M., Akbar, S. S., ... & Akour, I. A. (2021). IoT for smart cities: Machine learning approaches in smart healthcare—A review. *Future Internet*, *13*(8), 218.

[40] Mirani, A. A., Velasco-Hernandez, G., Awasthi, A., & Walsh, J. (2022). Key challenges and emerging technologies in industrial IoT architectures: A review. *Sensors*, *22*(15), 5836.

[41] Domínguez-Bolaño, T., Campos, O., Barral, V., Escudero, C. J., & García-Naya, J. A. (2022). An overview of IoT architectures, technologies, and existing open-source projects. *Internet of Things*, *20*, 100626.